

IN THE



UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED

APPLICANTS:

PAUL C. KOCHER et al.

SEP 2 7 2004

SERIAL NO.:

10/005,105

Technology Center 2100

FILING DATE:

December 03, 2001

TITLE:

DIFFERENTIAL POWER ANALYSIS METHOD AND

APPARATUS

EXAMINER:

not yet known

CONFIRMATION NO:

1675

GROUP ART UNIT:

2132

ATTY. DKT. NO.:

44424162-8721

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria,

VA 22313-1450, on the date shown below:

Dated: 22 Solember 2004

Michael C. Martensen, Reg. No. 46,901

MAIL STOP AMENDMENT COMMISSIONER FOR PATENTS P.O. BOX 1450 ALEXANDRIA, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

SIR:

Pursuant to the provisions of 37 CFR 1.56 and 1.97-1.98, Applicants hereby cite the references listed on the accompanying substitute PTO-1449 without inferring or suggesting, but instead expressly disclaiming any inference or suggestion, that any more pertinent reference exists. The filing of the information disclosure statement shall not be construed as a representation that a search has been made (37 CFR §1.97(g)), or an admission that the

Best Available Copy

information cited is, or is considered to be, material to patentability. Applicants enclose herewith copies of the all cited references. All references are in the English language.

The Commissioner is authorized to charge any fees required in connection with the submission of this IDS to deposit account number 19-3140. This sheet is being submitted in duplicate.

Respectfully submitted,

22 John 6 1200 A

Michael C. Martensen Registration No. 46,901 Attorney under Rule 34(a)

SONNENSCHEIN NATH & ROSENTHAL LLP P.O. Box 061080 Wacker Drive Station, Sears Tower Chicago, IL 60606-1080 Tel.: (415) 882-0357

,

enclosures

PTO/SB/08a (08-03)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substit	RADE UNITED TO THE PROPERTY OF		Complete if Known			
			Application Number	10/005,105		
INFC	DRMATION DISC	LOSURE	Filing Date	December 3, 2001 RECEIVE		
STA	TEMENT BY API	PLICANT	First Named Inventor	Paul C. Kocher		
			Group Art Unit	2132 SEP 2 7 20	201	
(use as many sheets as necessary)			Examiner Name	not vet known	Γ°	
Sheet	1 of	3	Attorney Docket Number	44424162-8721 ** Chinology Center	r 21 00	

	U.S. PATENT DOCUMENTS								
Examiner Initials*	Cite Document Number No. 1 Number-Kind Code ^{2 (if known)}		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear				
	AA	US-4,203,166	05/13/1980	Ehrsam et al.					
	AB	US-4,214,126	07/22/1980	Wipff					
	AC	US-4,243,890	01/06/1981	Miller et al.	·				
	AD	US-5,241,598	08/31/1993	Raith					
	AE	US-5,297,201	03/22/1994	Dunlavy					
	AF	US-5,341,423	08/23/1994	Nossen					
	AG	US-5,369,706	11/29/1994	Latka					
	AH	US-5,412,379	05/02/1995	Waraska et al.					
	Al	US-5,420,925	05/30/1995	Michaels					
	AJ	US-5,544,086	08/06/1996	Davis et al.					
	AK	US-5,552,776	09/03/1996	Wade et al.					
	AL	US-5,559,887	09/24/1996	Davis et al.					
	AM	US-5,600,324	02/04/1997	Reed et al.					
	AN	US-5,633,930	05/27/1997	Davis et al.					
	AO	US-5,733,047	03/31/1998	Furuta et al.					
	AP	US-5,761,306	06/02/1998	Lewis					

FOREIGN PATENT DOCUMENTS									
Examiner Initials*	Cite No.1	Foreign Patent Number Country Code ³ Number ⁴ Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ₆			
	AQ	EP 0 529 261 A2	03/03/1993	IBM Corp.					
	AR	EP 0 582 395 A2	02/09/1994	Digital Equipment Corp					
		,				늗			
——————————————————————————————————————						占			
Examii Signat				Date Considered	1				

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unquie citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO					Complete if Known			
				Application Number		10/005,105		
INFO	RMATI	ON DISCLOSURE	i	Filing Date		December 3, 2001		
STAT	TEMEN	T BY APPLICANT		First Named Inventor		Paul C. Kocher RECEIVED		
1					Group Art Unit		2132	
l I -					Consider Name		ow SEP 2 7 2004	
Sheet	2	of 3			ocket Number	44424162	-8721	
							-8721 Technology Center 210	
	1		J.S. PA	TENT DO	CUMENTS			
Examiner	Cite	Document Number		ation Date	Name of Pate		Pages, Columns, Lines, Where Relevant Passages or	
Initials*	No. ¹	Number-Kind Code ^{2 (if known)}		DD-YYYY	Applicant of Cited	Document	Relevant Figures Appear	
PE	AS.	US-5,778,065)7/1998	Hauser, et al.			
0	A15	US-5,796,836 US-5,995,629		18/1998 30/1999	Markham, Thom Reiner	ias R.		
2 %	CON H	US-5,995,629	11/3	00/1999	Reillei			
SEP 2 h	9					<u> </u>		
A	1,628		-					
A TRAI	EMP							
	+		-					
-								
		FO	DREIGN	PATENT D	OCUMENTS		Pages, Columns, Lines,	
Examiner Initials*	Cite No.1	Foreign Patent Number		Publication Da MM-DD-YYY			Where Relevant Passages or T6	
IIII(idiS		Country Code ³ Number ⁴ Kind Code ⁵ (if	known)	WINI-DD-171	Applicant of Ole		Relevant Figures Appear	
		<u> </u>						
					-			
Evamir	or.	,			Dat	10		

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unque citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. 6 Applicant is to place a check mark here if English language Translation is attached.

Signature

Considered

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2. Alexandria, VA 22313-1450.

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control no.

Substitu	te for form 1449B/PT	O		Complete if Known		
				Application Number	10/005,105	
INFO	RMATION DI	SCI	OSURE	Filing Date	December 3, 2001	
ିଂSTA1	TEMENT BY	APP	LICANT	First Named Inventor	Paul C. Kocher	
JA [3]				Group Art Unit	2132	
	(use as many	sheet	s as necessary)	Examiner Name	not yet known	
Sheet	3	of	3	Attorney Docket Number	44424162-8721	

	OTHER ITEMS - NON PATENT LITERATURE DOCUMENTS						
Examiner Initials*	CiteN o.1	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.					
	AV	American National Standards for Financial Services, secretariat - American Bankers Association (ANS/ABA x9.24-1997), "Financial Services Key Management," approved April 6, 1992, American National Standards Institute; pgs. 1-71					
	AW	JUENEMAN, Robert R., "Analysis of Certain Aspects of Output Feedback Mode", Satellite Business Systems, 1998; pgs. 99-127					
	AX	BAUER, Friedrich L., "Cryptology - Methods and Maxims", Technical University Munich, 1998; pgs. 31-48					
	AY	CONNOR, Doug (Technical Editor), "Cryptographic Techniques - Secure Your Wireless Designs", 01/18/96; pgs. 57-68					
	AZ	HORNAUER et al., "Markov Ciphers and Alternating Groups," Eurocrypt 91, 1991; pgs. 453-460					
	BA	KOBLITZ, "A Course in Number Theory and Cryptography" 2e, 1994, Chapter III; pgs. 53-77					
	BB	LAI et al., "Markov Ciphers and Differential Cryptanalysis," Eurocrypt 91, 1991; pgs. 17-38					
	ВС	HACHEZ et. al. "Timing Attack: What Can Be Achieved By A Powerful Adversary?" 1999					
	BD	KOCHER, Paul C., "Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks," Report 7 December 1995; pgs. 1-6					
	BE	KALISKI, Burt, "Timing Attacks on Cryptosystem," RSA Laboratories, Bulletin, Number 2, January 23, 1996					

Examiner	Date	
Signature	Considered	

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO:

Commissioner for Patents, Washington, DC 20231.

^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² Applicant is to place a check mark here if English language Translation is attached.